UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,072	10/31/2001	Richard L. Schertz	10016864-1	3588

7590 03/30/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/002,072	SCHERTZ ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In view of the Appeal Brief filed on 1/17/06, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.1 1 1 (if this Office action is non-final) or a reply under 37 CFR 1.1 13 (if this Office action is finall; or,

(2) request for reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, aïdavits (37 CFR 1.130, 1. 131 or 1.132) or other evidence are permitted. See 37 CFR 1.193 (b)(2).

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

2. Claims 1-29 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-5, 15-17 and 22-24 are rejected under 35 U.S.C. 102(b) as being anticipated by "Doctor Web for Windows (workstation) published by DialogueScience, Inc., 1999 (hereinafter Doctor Web).

As per claims 1 and 15:

Doctor Web teaches a computer and a method comprising:

an operating system controlling a computer resource; (Page 1, paragraph 1) and

an intrusion detection system integrated with the operating system and operable to monitor the computer resources to detect and prevent intrusion attempts. (Page 1, paragraph 1; ...one of the world's most clever memory resident monitors -"Spider Guard", deeply integrated into the operating system, which practically excludes any possible intrusion ...)

As per claims 2-3, 16-17 and 23:

Doctor Web teaches all the subject matter as discussed above. In addition, Doctor Web further discloses a computer and a method wherein the computer resource is selected from the group consisting of data storage system, input/output system, a networking system, an application program execution environment, and interfaces to peripheral devices. (Page 2, DrWeb for Windows 95/98/NT scan objects such as drives, folders, and even individual files)

As per claims 4-5 and 24:

Doctor Web teaches all the subject matter as discussed above. In addition, Doctor Web further discloses a computer and a method comprising an anti-virus system integrated with the operating system and operable to monitor the data storage system,

input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus. (Page 1, paragraph 1; ... memory resident monitors -"Spider Guard", deeply integrated into the operating system, which practically excludes any possible intrusion of malicious code, i.e. virus, worm, Trojan ...)

As per claim 22:

Doctor Web teaches a method comprising:

executing an OS-integrated anti-virus system; (Page 1, paragraph 1) and

monitoring at least one computer resource to detect the presence of at least one virus. (Page 1, paragraph 1; ... memory resident monitors -"Spider Guard", deeply integrated into the operating system, which practically excludes any possible intrusion of malicious code, i.e. virus, worm, Trojan program into your computer)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 10-14 and 25-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Doctor Web for Windows (workstation) published by DialogueScience, Inc., 1999 (hereinafter Doctor Web) in view of Walsh et al. (hereinafter Walsh) United States Letter Patent Number 5,856,481.

As per claims 10 and 25:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose an anti-virus system comprises a module operable to prevent reassembly of a virus.

Walsh in analogous art, however, discloses an anti-virus system comprises a module operable to prevent reassembly of a virus. (Col. 2, lines 63-67; Col. 3, lines 20-22)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Doctor Web to include an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Walsh (Abstract) in order to have a system that provides protection from infection or damage by a virus and advise the possible danger of spreading the virus.

As per claims 11 and 26:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose an anti-virus system comprises a module operable to recognize a virus. Walsh in analogous art, however, discloses an anti-virus system comprises a module operable to recognize a virus. (Col. 7, lines 25-41)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Doctor Web to include an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Walsh (Abstract) in order to have a system that provides protection from infection or damage by a virus and advise the possible danger of spreading the virus.

As per claims 12 and 27:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose an anti-virus system comprises a module operable to prevent storage of a virus. Walsh in analogous art, however, discloses an anti-virus system comprises a module operable to prevent storage of a virus. (Col. 3, lines 38-42)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Doctor Web to include an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as

suggested by Walsh (Abstract) in order to have a system that provides protection from infection or damage by a virus and advise the possible danger of spreading the virus.

As per claims 13 and 28:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose an anti-virus system comprises a module operable to prevent transmission of a virus. Walsh in analogous art, however, discloses an anti-virus system comprises a module operable to prevent transmission of a virus. (Col. 10, lines 7-12)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Doctor Web to include an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Walsh (Abstract) in order to have a system that provides protection from infection or damage by a virus and advise the possible danger of spreading the virus.

As per claims 14 and 29:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose a computer wherein the anti-virus system comprises a module operable to prevent execution of a virus. Walsh in analogous art, however, discloses an anti-virus system comprises a module operable to prevent execution of a virus. (Col. 2, lines 63-67; Col. 3, lines 20-22)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the device disclosed by Doctor Web to include an anti-virus system integrated with the operating system and operable to monitor the data storage system, input/output system, networking system, application program execution environment, and interfaces to peripheral devices to detect and report the presence of at least one virus. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Walsh (Abstract) in order to have a system that provides protection from infection or damage by a virus and advise the possible danger of spreading the virus.

7. Claims 6-9 and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Doctor Web for Windows (workstation) published by DialogueScience, Inc., 1999 (hereinafter Doctor Web) in view of Holland, III et al. (hereinafter Holland) United States Letter Patent Number 6,851,061.

As per claims 6 and 18:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose a computer and a method wherein intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames.

Holland in analogous art, however, discloses intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. (Figure 4; Col. 2, lines 26-27 and lines 35-36; Col. 5, lines 25-27; Col. 6, lines 29-61)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the computer and the method disclosed by Doctor Web to include intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Holland (Col. 2, lines 17-19) in order to have a scalable solution providing packet traffic for network intrusion detection and analysis.

As per claims 7 and 19:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose a computer and a method wherein the intrusion detection system is integrated with a networking stack of the networking system above the network layer operable to access reassembled fragments.

Holland in analogous art, however, discloses an intrusion detection system is integrated with a networking stack of the networking system above the network layer operable to access reassembled fragments. (Figure 4; Col. 5, lines 9-22 and lines 29-46; Col. 6; lines 29-61)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the computer and the method disclosed by Doctor Web to include intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. This modification would have been obvious because a person having ordinary skill in the art

would have been motivated to do so as suggested by Holland (Col. 2, lines 17-19) in order to have a scalable solution providing packet traffic for network intrusion detection and analysis.

As per claims 8 and 20:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose a computer and a method wherein the intrusion detection system is integrated with a networking protocol stack of the networking system above the transport layer.

Holland in analogous art, however, discloses an intrusion detection system is integrated with a networking protocol stack of the networking system above the transport layer. (Figure 4; Col. 6, lines 29-61; Col. 7, lines 17-42)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the computer and the method disclosed by Doctor Web to include intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Holland (Col. 2, lines 17-19) in order to have a scalable solution providing packet traffic for network intrusion detection and analysis.

As per claims 9 and 21:

Doctor Web teaches all the subject matter as discussed above. Doctor Web does not explicitly disclose a computer and a method wherein the intrusion detection system

is integrated with a networking stack of the networking system between the network layer and the transport layer and between the transport layer and the application layer.

Holland in analogous art, however, discloses an intrusion detection system is integrated with a networking stack of the networking system between the network layer and the transport layer and between the transport layer and the application layer. (Figure 4; Col. 6, lines 29-61; Col. 7, lines 17-42)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the computer and the method disclosed by Doctor Web to include intrusion detection is integrated with a networking stack of the networking system above the link layer operable to access raw network frames. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Holland (Col. 2, lines 17-19) in order to have a scalable solution providing packet traffic for network intrusion detection and analysis.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
3/24/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER